Hastings Communications and Entertainment Law Journal

Volume 32 | Number 3 Article 2

1-1-2010

Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages

Sarah Salter

Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages

by
SARAH SALTER♦

> Socrates described what would be lost to human beings in the transition from oral to written culture. Socrates' protests . . . are notably relevant today as we and our children negotiate our own transition from a written culture to one that is increasingly driven by visual images and massive streams of digital information.[1]

I. Introduction

Privacy laws in the United States have been enacted to control both government investigation into private lives and to deter

♦ Sarah Salter, Professor of Law, New England Law | Boston; A.B. Radcliffe 1962,: J.D. Georgetown University Law Center, 1970. Courses taught include Internet Law, Computer Law, Tax, and Business Organizations.

1. MARYANNE WOLF, PROUST AND THE SQUID: THE STORY AND SCIENCE OF THE READING BRAIN 19 (Harper Collins 2007).

intrusions by private persons.[2] Communications between private persons have often been targeted for such investigation and intrusion.[3] United States federal law provides more protection

2. There are both Constitutional and statutory federal privacy protections. Constitutional protection most relevant to our examination is based on the Fourth Amendment to the United States Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. As will be important to note in connection with *United States v. Steiger*, Constitutional protection can only be invoked against the Government as the alleged intruder, not for privacy intrusions by private persons. 318 F.3d 1039 (11th Cir. 2003) (discussed *supra* notes 125–39). The Fourteenth Amendment, through its due process clause, makes the search and seizure provisions applicable to state defendants. Mapp v. Ohio, 367 U.S. 643, 655 (1961).

Statutory privacy protection for communications that will be primarily examined in this article is that provided by the Electronic Communications Privacy Act ("ECPA") of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C.A. §§ 2510–22, 2701–12, 3121–27 (2006 & Supp. 2008)). Title I of the ECPA, and its predecessors, will herein be termed the Wiretap Act, 18 U.S.C. §§ 2510–22. Title II of the ECPA will be referred to as the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–12. Both the Wiretap Act and the SCA deal with access to the content of communications, and are the focus of this article. By contrast, less protection is provided when law enforcement officials seek to access "addressing" information under Title III of the ECPA, which is usually known as the Pen Register Act, 18 U.S.C. §§ 3121–27. The analogy has been to postal access: access to the contents of sealed letters usually requires court supervision under the warrant upon probable cause procedure, but information on the outside of the envelope (addresses, postmarks) were not protected as material in which there is a "reasonable expectation of privacy." The Pen Register Act is only tangentially examined.

Additionally, the special provisions of the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–63 (2006), will not be examined. Many states have also enacted privacy protections; courts when applying those state laws often consider interpretations of parallel provisions in the federal statutes, so several state statutes will be discussed, although a comprehensive review is beyond the scope of this article. Both the Wiretap Act and the Stored Communications Act provide for civil actions to recover damages for unlawful access to protected communications. 18 U.S.C. §§ 2520, 2707 (2006).

3. In the leading case on communications privacy, Justice Stewart developed the "reasonable expectation of privacy" test in finding that a man's Fourth Amendment right to privacy was violated when FBI agents "attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls." Katz v. United States, 389 U.S. 347, 348–49 (1967). Justice Stewart explained:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

Id. at 351 (citations omitted).

against intrusion for communications of the human voice in the process of transmission than it does for data transmissions such as email and text messages.[4] It provides even less protection for data communications in digital or electronic storage.[5] As part of the dramatic increase in use of "cloud computing," where remote servers provide hardware and software for even such basic tasks as word processing, more and more data, including communications, will be stored on third-party servers.[6] The foundation of different treatment for stored communications, as well as the effect it will have on cloud computing, is the focus of this article.

In examining the scope and limitations on privacy protections for communications, courts have applied the U.S. Constitution, the federal Electronic Communications Privacy Act ("ECPA"), and other state and federal privacy statutes. Both legislatures and courts have limited privacy protections where other interests are found to conflict.[7] The Fourth Amendment to the United States Constitution has long provided protection for communications stored in either document form or electronic form, so long as the storage was within the home, or another place recognized by general search and seizure law as a location in which the individual had a reasonable expectation of privacy.[8] However, electronic communications are not so physically confined, whether stored or in transmission, therefore, Congress and the states have provided statutory privacy protections that echo, overlap, and extend Constitutional mandates.

The federal ECPA distinguishes between communications in which the human voice is transmitted and other data transmissions, such as email and text messages.[9] The greater protection for voice

4. Under the Wiretap Act, some protection is provided for all communications transmitted by wire, both data and voice; however, speech communications, defined as "oral" and "aural" in 18 U.S.C. § 2510, are protected by the suppression remedy under 18 U.S.C. § 2515, but data communications are not.

5. Under the SCA, communications that are stored, rather than in transmission, are not protected by a suppression remedy, process for access is less onerous, and statutory civil damages for violations are less generous. *See infra* Part II.A for greater discussion of differences between the Wiretap Act and the SCA.

6. "Cloud computing" is the popular term referring to the business model of providing use of hardware and software as a service over the internet. Rachael King, *How Cloud Computing Is Changing the World*, BUS. WK., Aug. 4, 2008, *available at* http://www.businessweek.com/technology/ content/aug2008/tc2008082_445669.htm.

7. "Where a careful balancing of governmental and private interests suggests that the public interest is best served by a Fourth Amendment standard of reasonableness that stops short of probable cause, we have not hesitated to adopt such a standard." New Jersey v. T.L.O., 469 U.S. 325, 341 (1985).

8. U.S. CONST. amend. IV; *see also Katz*, 389 U.S. at 352–53.

9. 18 U.S.C. § 2510(1), (2), (12) (2006).

transmissions ends, however, when voice communications become stored as voicemail.[10] The statutory concept of storage is complex and its application results in different levels of protection.[11] Only some communications that are stored in digital form may be in electronic storage, as narrowly defined under the federal Stored Communications Act ("SCA").[12] Further complicating the interpretation of the SCA, modern technology for transmitting emails and text messages involves ephemeral periods of storage in the process of transmission.[13] Similarly, the point at which a transmitted communication becomes finally "stored" has been an issue.[14]

Initially, this article compares specific statutory language to show that law enforcement officers seeking to intercept communications in transmission must make a stronger showing to obtain court permission than those seeking stored communications. The private remedy against violators for privacy intrusions prohibited under the SCA likewise is also described in Section II and is shown to be a lesser deterrent.

After setting out the statutory framework, Section III discusses cases that provide specific guidance on whether a communication is stored or in transit, and on issues that have been litigated when some

10. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act amended § 2703 of the ECPA to place stored wire communications, that is, voicemail, within the ECPA provisions that apply to stored electronic communication, such as e-mails. USA PATRIOT Act of 2001 § 209, Pub. L. No. 107-56, 115 Stat. 272, 283; *see also supra* note 5.

11. If a message is stored on an "electronic communications system" ("ECS") for 180 days or less, the message is protected from disclosure by a federal search warrant. 18 U.S.C. § 2703(a) (2006). However, a message stored either on an ECS for over 180 days or on a "remote computing service" ("RCS") is only protected by a subpoena or court order. 18 U.S.C. § 2703(a)–(b) (2006). An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications . . . ." 18 U.S.C. § 2510(15) (2006). An RCS is any service which provides to users "computer storage or processing services by means of an electronic communications system . . . ." 18 U.S.C. § 2711(2).

12. "Electronic storage" is narrowly defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (2006). The Department of Justice takes the position that, where an email is acquired from post-transmission storage, it is no longer in "electronic storage," as protected by the SCA. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 123–24 (2009) [hereinafter DOJ MANUAL], *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

13. The intermediate storage of information in the process of transmission raises this issue in *United States v. Councilman* (*Councilman I*), 418 F.3d 67, 70 (2005).

14. *See infra* notes 81–86.

form of storage occurs during the process of transmission. This section then analyzes the case law developing earmarks for classification within the categories of stored communication protected by the SCA. Next, Section III compares criminal cases, where suppression of evidence is sought, to cases brought under the civil claims provisions. It also notes the inconsistencies and limitations on privacy protection for communications thus developed. First Amendment cases and the application of freedom of information statutes have also limited privacy protections for communications, and Section III includes a discussion of them for additional perspective in developing alternatives to the current statutory framework.

This article, comparing legal protections for stored communications to those for in-transit communications, was initially begun as a paper for the Media in Transition Conference 6, which gathered a cross-disciplinary group of scholars and professionals to explore the theme "Stone and Papyrus: Storage and Transmission."[15] This article concludes by suggesting that a reexamination of the legislative treatment of the SCA is appropriate, given the impact of "cloud computing" and digital technologies that preserve vast stored reservoirs of personal communications and other data, and make that information available for rapid and efficient transmission, search, and retrieval.[16] Specific changes addressed include a proposal for

15. Media in Transition: Mission, http://web.mit.edu/comm-forum/mit6/ (last visited Nov. 5, 2009). The conference planners based the theme on a canonical text in media studies in which Harold Innis distinguishes between time-based and space-based media. HAROLD INNIS, THE BIAS OF COMMUNICATION 33 (University of Toronto Press 1999) (1951). Innis argues that stone tablets are durable, and thus time-based, but are heavy so have little spatial impact. HAROLD INNIS, EMPIRE AND COMMUNICATIONS 26 (Dundurn Press 2007) (1950). Space-based media, such as papyrus and paper, are seen as more powerful, though fragile, because they can be diffused widely, creating connections over space. *Id.* at 27. Innis was writing in the years immediately after World War II, with a background as an economic historian specializing in such traditional work as a history of the Hudson's Bay Company. *Id.* at 13. The amazing impact of technology in the years since shows a dazzlingly rapid set of transitions as we consider the time and spatial dimension changes from stone tablets to papyrus to printing press to radio to digital transmission.

16. In 1997, it was found that:

> the United States digitally stores more than 400 billion documents, with 72 billion new documents being added each year. Digital document storage and retrieval will become more and more prevalent. This is, in part, driven by a change in cost structure. The cost of digital data storage has decreased to the point where digital forms are the least expensive means to store most of the information which traditionally would have been printed or microfilmed.

extending the exclusionary remedy to violations of the SCA and a proposal for repealing the civil claim remedy.

II. Statutory Framework

Privacy law in the United States has Constitutional roots. The Fourth Amendment secures people "in their persons, houses, papers, and effects, against unreasonable searches and seizures," and penumbral protection of privacy has been recognized under that and other amendments of the Bill of Rights.[17] However, the Fourth

ATP Focused Program Competition 97-04 Digital Data Storage, Advanced Technology Program, National Institute of Standards and Technology (1997), *available at* http://www.atp.nist.gov/press/97-04dds.htm.

17. U.S. CONST. amend. IV. *See also supra* note 2.

> The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."
>
> The Fourth and Fifth Amendments were described . . . as protection against all governmental invasions "of the sanctity of a man's home and the privacies of life." . . . We have had many controversies over these penumbral rights of "privacy and repose." These cases bear witness that the right of privacy which presses for recognition here is a legitimate one.

Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965) (citations omitted). English precedent has been cited for the principle embodied in the Fourth Amendment. The phrase "the house of everyone is to him as his castle and fortress" appears in *Semayne's Case*, (1603) 77 Eng. Rep. 194, 195 (K.B.). However, modern historians suggest that the Fourth Amendment went well beyond existing English precedent in protecting privacy.

> The requirement that warrants uniformly limit their application to the persons and places specified—the cornerstone of the Fourth Amendment—transcended earlier guarantees by prohibiting discretionary searches rather than merely qualifying them. This view of the matter differs from traditional interpretations that characterize the Fourth Amendment . . . as little more than a hallowing of already existing English and American legal triumphs.

William Cuddihy & B. Carmon Hardy, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 WM. & MARY Q. 371, 372 (1980).

Amendment applies only to intrusions by government, and its application is weak and uncertain as applied outside the physical home to information stored in electronic form rather than as "papers."[18] Thus, Congress enacted statutory protections for communications in 1934,[19] after telephone technology raised privacy issues.[20] Congress further developed the statutory framework in 1968,[21] and most recently passed the ECPA in 1986.[22]

Under the different sections of the ECPA, the familiar procedure of requiring probable cause for a search warrant is applicable to wiretap surveillance of communications in transmission,[23] while less stringent procedures are needed for law enforcement agents to gain access to stored electronic communications.[24] However, employers generally have been allowed to access employee email and other internet usage stored on or transmitted through employer-provided equipment outside of court proceedings and judicial supervision.[25]

18. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209–13 (2004) [hereinafter Kerr, *A User's Guide*].

19. The Federal Communications Act, enacted in 1934, provided: "No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person." 47 U.S.C. § 605(a) (1934).

20. In *Olmstead v. United States*, 277 U.S. 438, 466 (1928), the Supreme Court held that wiretapping did not violate the Fourth Amendment.

21. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 outlined protection for electronic surveillance, providing for court supervision: judges could authorize wiretap warrants upon a showing of "probable cause" that an individual is, has, or is preparing to break any of the laws listed in the act. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197. 218–21.

22. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848; *see supra* note 2.

23. 18 U.S.C. §§ 2516–18 (2006).

24. 18 U.S.C. § 2703(c) (2006).

25. "Although e-mail communication, like any other form of communication, carries the risk of unauthorized disclosure, the prevailing view is that . . . confidential information [may be communicated] through unencrypted e-mail with a reasonable expectation of confidentiality and privacy." *In re* Asia Global Crossing, LTD., 322 B.R. 247, 256 (Bankr. S.D.N.Y. 2005) (collecting authorities). In determining whether an employee had an expectation of privacy in emails sent or received on her employer's computer or email system, a court should consider the following four factors:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

Courts and legislatures in the United States have also recognized a countervailing public interest in making public some communications that would otherwise be protected as private. First Amendment claims have protected people from liability for disclosing private information relevant to public issues, even when the information was taken from unlawfully intercepted transmissions.[26] Freedom of information acts at the federal and state levels have been invoked to compel the release of stored information created by public officials.[27] This article will primarily deal with the ECPA, rather than Constitutional claims and state privacy legislation.

A. Privacy Protections for Communications Intercepted in Transmission Under the Wiretap Act and Under the SCA

In-transit communications receive more protection from interception than stored communications in three ways: (1) the more

Id. at 257.

26. *See* Bartnicki v. Vopper, 532 U.S. 514, 535 (2001). In the long duel over truthful material released by Representative McDermott on a matter of public interest that was initially recorded unlawfully, though not by the Representative, the Circuit Court for the District of Columbia ultimately declined to rule on the scope of First Amendment protection, but a concurring opinion suggests strong support for its application:

> Although I agree that Representative McDermott's actions were not protected by the First Amendment and for that reason join Judge Randolph's opinion, I write separately to explain that I would have found the disclosure of the tape recording protected by the First Amendment under *Bartnicki v. Vopper*, had it not also been a violation of House Ethics Committee Rule 9, which imposed on Representative McDermott a duty not to "disclose any evidence relating to an investigation to any person or organization outside the Committee unless authorized by the Committee. Although the Court does not and need not reach the *Bartnicki* issue to resolve the matter before us, two previous panels in this case have held that the congressman's actions were not protected by the First Amendment. I believe it is worth noting that a majority of the members of the Court—those who join Part I of Judge Sentelle's dissent—would have found his actions protected by the First Amendment.

Boehner v. McDermott, 484 F.3d 573, 581 (2007) (Griffith, Cir. J., concurring).

27. 5 U.S.C.A. § 552 (West 2008); U.S. Department of Justice: General Information about the Freedom of Information Act, http://www.usdoj.gov/oip/index.html (last visited Nov. 5, 2009) (explaining that the Freedom of Information Act "applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Each state has its own public access laws that should be consulted for access to state and local records."). *See also* Joe Swickard, *Steps in the Text Message Scandal*, THE DETROIT FREE PRESS, Mar. 10, 2009, *available at* http://www.freep.com/article/20090310/NEWS01/903100351/; M. Elrick, *Judge Rules that Kilpatrick, Beatty Texts are Public Record*, THE DETROIT FREE PRESS, Mar. 4, 2009, *available at* http://www.freep.com/article/20090304/NEWS01/90303093/.

stringent requirements for obtaining a warrant for wiretaps then for accessing stored communications; (2) the absence of an exclusionary rule for evidence unlawfully obtained in violation of the SCA or for data communications unlawfully intercepted in transmission; and (3) the lesser provision for statutory damages in civil claims for violation of the SCA than of the Wiretap Act.

1. Lawful Access to Communications Under the Wiretap Act and Under the SCA

The Wiretap Act, as amended by the ECPA, makes it illegal for anyone to "intentionally intercept . . . any wire, oral, or electronic communication."[28] "Intercept" is defined in the Wiretap Act as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[29] However, a procedure for allowing interception under impartial judicial supervision[30] has been provided for the investigation of certain enumerated serious crimes.[31] Significantly, the Wiretap Act's procedure is more restrictive than the usual Fourth Amendment warrant procedure for a lawful search or seizure, and has thus been described as a "super" warrant.[32] Under the Wiretap Act, a law enforcement officer may request a court to permit interception by an application that includes a sworn statement of facts, obtained from an independent investigation, to justify his belief that the interception should be permitted, including:

> (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) . . . a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, [and] (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted . . . .[33]

Further, the requesting officer must declare "whether or not other investigative procedures have been tried and failed or why they

28. 18 U.S.C.A. § 2511(1) (West 2008).
29. 18 U.S.C. § 2510(4) (2006).
30. 18 U.S.C. § 2518 (2006).
31. 18 U.S.C. § 2516 (2006).
32. Kerr, *A User's Guide*, *supra* note 18, at 1232.
33. 18 U.S.C. § 2518(1)(b).

reasonably appear to be unlikely to succeed if tried or to be too dangerous."[34]

The judge reviewing the application may issue a time-limited order[35] permitting interception if it is found that

> (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit [the list of serious crimes referred to above]; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; [and] (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. . . .[36]

In contrast, the SCA addresses access to protected stored communications, rather than interception of in-transit communications.[37] Penalties are set forth for whoever

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage . . . .[38]

However, there is no crime, or parallel civil action, where the access is "authorized."[39] Authorization may be granted by persons other than a party to the communication, including the provider of the wire or electronic communications service, by a user of the service with respect to a communication of that user or intended for that user, or by a process significantly less protective than the process for interception under the Wiretap Act, as described above.[40]

The process for obtaining authorization to obtain stored electronic communications requires court-supervised warrant-based access to communications stored for 180 days or less, although privacy safeguards are fewer than those for communications covered

34. 18 U.S.C. § 2518(1)(c).
35. 18 U.S.C. § 2518(5).
36. 18 U.S.C. § 2518(3).
37. 18 U.S.C. § 2701 (2006).
38. 18 U.S.C. § 2701(a).
39. 18 U.S.C. § 2701(c).
40. *Id. See also supra* notes 32–36.

under the Wiretap Act.[41] Stored communications within a 180-day period may be accessed "pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offence under investigation or equivalent state warrant."[42] Those rules are less onerous than the wiretap "super" warrant procedure described above. The law enforcement investigator seeking access to the communications may obtain the warrant upon a probable cause showing that the material sought is likely to provide evidence of a crime,[43] and there is no specified list of crimes limiting the scope of such an order, unlike the list in the Wiretap Act.[44] The applicant is not required to show that other investigative procedures have been tried and have failed, or are unlikely to succeed, or are too dangerous. Congress has also instituted a reporting requirement for wiretap warrants,[45] mandating recordkeeping and public access to those records, but has not done so for access to stored communications.

If the communication has been in electronic storage for more than 180 days, it can be accessed by a governmental agent by obtaining a subpoena or court order merely upon a showing that "there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[46]

2. *Statutory Exclusion of Evidence Under the Wiretap Act and Under the SCA*

Both the Wiretap Act and the SCA contain strong civil enforcement remedies[47] in addition to imposing criminal sanctions for unlawful intrusions into the privacy of communications. However, most cases interpreting the Wiretap Act privacy protections have arisen in the criminal context, where suppression of evidence is sought on the ground that the interceptor violated the process set forth in the act.[48]

41. *Compare* 18 U.S.C. § 2703(a) (2006) *with* 18 U.S.C. § 2518.
42. 18 U.S.C. § 2703(a).
43. FED. R. CRIM. P. 41 (b), (c)(1) (2007).
44. 18 U.S.C. § 2516 (2006).
45. 18 U.S.C. § 2519 (2006).
46. 18 U.S.C. § 2703(b), (d) (2006).
47. 18 U.S.C. § 2520 (2006); 18 U.S.C. § 2707 (2006).
48. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 824 (2003) [hereinafter Kerr, *Lifting the "Fog"*].

The Wiretap Act contains a stringent rule excluding any unlawfully obtained wire or oral communication from use as evidence in any proceeding.[49] The absence of any such provision for unlawful access to stored communications or for unlawful interception of electronic communications that do not contain the human voice clearly signals an intent by Congress to treat such intrusions into privacy differently. However, the rationale for differentiating between the two is not so clear here as in other respects. Both statutes have powerful civil claims provisions, but the absence of an exclusionary remedy (or an injunctive remedy, as is provided under the Wiretap Act[50]) may suggest that Congress is more concerned that law enforcement officials will misuse wiretaps on communications containing the human voice than will unlawfully access data communications or stored communications. Alternatively, as in the other points of different treatment, it may suggest that Congress values the privacy interest in oral communications in transit more than privacy in data and stored communications. Similarly, following the line of analysis applied to Fourth Amendment protection against search and seizure, Congress may have determined that individuals have a higher expectation of privacy for oral communications in transit, as compared to data in transit and stored communications.

The legislative history of the ECPA of 1986 offers little guidance. There was much support in Congress for a comprehensive revision of the ECPA in 2000 that would have heightened privacy protections.[51] The bill, as reported out of committee, included extension of the suppression remedy to electronic non-voice communications in transit, and also to stored voicemail and email messages.[52] The

49. "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding . . . if the disclosure of that information would be in violation of this chapter." 18 U.S.C. § 2515 (2006).

50. 18 U.S.C. § 2521 (2006).

51. *House Committee Delays Adoption of Electronic Communications Privacy Act,* TECH L.J., Sept. 22, 2000, *available at* http://www.techlawjournal.com/privacy/20000922.asp.

52.

> Currently, only illegally obtained "wire and oral communications" are excluded from use as evidence by statute. H.R. 5018 would amend the "statutory exclusionary rule" to also exclude from use as evidence illegally intercepted "electronic communications" and illegally obtained "electronic communications in electronic storage," namely stored e-mail messages, resulting from violations [of] the Electronic Communications Privacy Act . . . .

Electronic Communications Privacy Act of 2000, H.R. REP. NO. 106-932, at 15–16 (2000).

proposal died as the Clinton administration ended, and was not revived the following year when terrorism concerns, raised by the events of September 11, 2001, drained support for privacy law extension.[53]

Scholars have urged that an exclusionary rule be adopted for unlawful intrusions into stored communications.[54] They argue that civil litigation has been the usual response to violations of the SCA, resulting in courts deciding on its interpretation in the context of

53. Sandra McKay, *The Evolution of Online Privacy: 2000–2003*, J. LEGAL, ETHICAL AND REG. ISSUES, at 4–5 (2003), *available at* http://findarticles.com/p/articles/mi_m1TOS/is_2_6/ ai_n25080548/?tag=content;col1.

> As the result of an FTC survey that found only 20 percent of all websites and less than half of the 100 most popular sites used industry-accepted fair information practices, such as letting users opt out, the agency called on Congress to protect consumers through laws that would establish standard practices for collection and use of online data. Legislators responded and an abundance of privacy bills were introduced into Congress during the years and months immediately preceding the events of September 11, 2001. After the 2000 Congressional session in which dozens of Internet privacy bills died in committee and others languished without any indication of being recommended for a full vote, the general conviction was that year 2001 could be the year for breaking the impasse over Internet privacy.
>
> Early 2001, privacy advocates, industry trade groups, and legislators alike believed that some federal government actions seemed unavoidable. Privacy advocates saw hope in the Senate's sudden shift to Democratic control . . . . Pres. Bush's decision to implement the medical privacy regulations approved late in the Clinton administration provided further expectations of federal action in the belief that it would heighten awareness of privacy issues. And the FTC remained a strong advocate of new federal laws on privacy. . . . The question for many industry executives had shifted from "will" there be new legislation to "what" issues will new laws address.
>
> . . .
>
> The heinous terrorist acts of September 11 marked a significant turning point in the debate over privacy. Such an event changes the balance between security and privacy, giving new weight to calls for broader government surveillance powers. Swept up in a tide of emotional fear and anger, the immediate response for most Americans was for greater security and protection from further attacks. In the face of potential catastrophic danger, most would choose to relinquish some privacy rights in favor of a safer, more secure world.

Id. (internal citations omitted).

54. *See generally* Michael S. Leib, *E-mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject A "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393 (1997); Kerr, *A User's Guide*, *supra* note 18, at 1241–42.

weighing the interests of a plaintiff claiming injury against interests of civil defendants.[55] In comparison, the interpretation of the Wiretap Act exclusionary rule has been litigated in the context of weighing a criminal defendant's civil liberties against intrusions by law enforcement officials.[56]

3. Statutory Damages for Violation of the SCA

Congress has also signaled that it places a higher value in preserving privacy for communications in transit as compared to stored communications in the provisions for civil damage claims provided under both acts.[57] Provisions for the awarding of attorneys' fees and punitive damages, as well as actual and statutory damages, create significant incentives for civil claims to deter unlawful access to stored communications and unlawful interception of in-transit communications. Statutory damages here are particularly important given the uncertainty and costs of proving actual damages. However, the statutory damages provision for violations of the SCA sets a minimum recovery for a violation at $1,000, although if actual damages are greater they would be available.[58] If there is an interception in violation of the Wiretap Act, however, statutory damages are set at $10,000 per violation or $100 per day of the continuing violation, whichever is greater.[59]

4. Treatment of Different Types of Communications Under the ECPA

The suppression remedy granted under the Wiretap Act,[60] which prohibits the use of unlawfully obtained wiretap evidence being used in trial, is not made available to stored communications or to non-voice communications in transit, as noted above. The statutory language makes clear that the protection afforded by the suppression remedy is limited to a "wire or oral communication."[61] In the definitional provision of the statute, electronic communication is expressly distinguished as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, *but*

55. Leib, *supra* note 54, at 436; Kerr, *A User's Guide*, *supra* note 18, at 1241–42.
56. *See* Kerr, *Lifting the "Fog," supra* note 48, at 829.
57. 18 U.S.C. §§ 2520, 2707, 2712 (2006).
58. 18 U.S.C. § 2707(c) (2006).
59. 18 U.S.C. § 2520(c)(2)(B) (2006).
60. 18 U.S.C. § 2515 (2006).
61. *Id.*

does not include—(A)any wire or oral communication . . . ."[62] An oral communication is defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication . . . ."[63] A wire communication is defined as:

> Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.[64]

An aural transfer is defined as "a transfer containing the human voice at any point between and including the point of origin and the point of reception . . . ."[65] The legislative history clarifies that an "oral" communication is an utterance by the human voice that travels by sound waves and a "wire" communication is an utterance carried as an electrical impulse by wire or other device: "An oral communication is an utterance by a person under circumstances exhibiting an expectation that the communication is not subject to interception, under circumstances justifying such an expectation. In essence, an oral communication is one carried by sound waves, not by an electronic medium."[66]

In describing and protecting oral communications, the ECPA of 1986 thus incorporated the standard for privacy protection under the Fourth Amendment that the U.S. Supreme Court articulated in *Katz v. United States* in 1967, with respect to eavesdropping outside the Fourth Amendment-protected physical confines of the home.[67] In that case, a device had been placed to pick up the content of voice communications uttered by a speaker in a public phone booth.[68] The recorded evidence obtained was excluded when the court determined

62. 18 U.S.C. § 2510(12) (2006) (emphasis added).
63. 18 U.S.C. § 2510(2) (2006).
64. 18 U.S.C. § 2510(1) (2006).
65. 18 U.S.C. § 2510(18) (2006).
66. S. REP. NO. 99-541, at 13 (1985), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3567.
67. Katz v. United States, 389 U.S. 347, 351 (1967).
68. *Id.* at 348.

that one can have a reasonable expectation of privacy in activities beyond the home.[69]

In recognition that human voice communications were being carried by technological means well beyond the copper wire of original telephones, and seeking to protect those voice communications as well, the ECPA protected "wire" communications, extending the definition to include:

> the whole of a voice telephone transmission even if part of the transmission is carried by fiber optic cable or by radio—as in the case of cellular telephones and long distance satellite or microwave facilities. The conversion of a voice signal to digital form for purposes of transmission does not render the communication non-wire. The term "wire communication" includes existing telephone service, and digitized communications to the extent that they contain the human voice at the point of origin, reception, [sic] or some point in between. A private telephone system established by a company whose activities affect interstate commerce, would also be covered.[70]

Thus, the statute protects transmissions of content produced by the human voice from interception with the powerful exclusionary rule, but does not offer that protection to content in written or other non-oral form, whether in transmission or as stored communications. Initially, the ECPA had extended the protection for voice communication to stored "voice mail,"[71] but that protection was removed in the USA PATRIOT Act[72] to allow wider surveillance in the aftermath of the events of September 11, 2001.[73]

69. *Id.* at 361 ("The rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'") (Harlan, J., concurring).

70. S. REP. NO. 99-541, at 12.

71. The Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks amended subparagraph (D) to specify that wire communications in storage like voice mail, remain wire communications, and are protected accordingly. *Id.*

72. The USA PATRIOT Act amended § 2703 of the ECPA to place stored wire communications, that is, voice mail, within the ECPA provisions that apply to stored electronic communication such as e-mails. USA PATRIOT Act of 2001 § 209, Pub. L. No. 107-56, 115 Stat. 272, 283.

73. Peter P. Swire, *Katz is Dead. Long Live Katz.*, 102 MICH. L. REV. 904, 911, 915 (2004).

The SCA does protect messages in electronic storage, but defines that category narrowly so that not all stored materials receive protection. "'[E]lectronic storage' means—(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication . . . ."[74]

The statutory distinctions that create differences in protection depend on the characterization of the storage provider and the nature of the materials. The statute sets up two categories of third parties holding stored communications, the "electronic communications service" and the "remote computing service."[75] The essential distinction between the two is that, while a remote computing service may hold a stored communication, it is doing so to provide operations on data rather than holding it in the context of the transmission itself. The concept originally was designed to cover electronic data sent by its owner to a third party who would provide services, such as accounting, database storage, and management that, under the state of technology in 1986, would be beyond the capacity of most business computers.[76] In 2010, it would presumably cover "Web 2.0" and

74. 18 U.S.C. § 2510(17) (2006).

75. The term "remote computing service" is defined in 18 U.S.C. § 2711(2) of the SCA and "electronic communication service" is defined in 18 U.S. C. § 2510(15) of the Wiretap Act. The distinction determines who may lawfully consent to disclosure of the message under 18 U.S.C. § 2701(b)(3): a message held by an ECS can lawfully be disclosed without a warrant only to the originator and the intended recipient, while a message held in an RCS can lawfully be disclosed to the subscriber to the service as well.

The legislative history of the term "remote computing service," provides a more detailed explanation:

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.

S. REP. NO. 99-541, at 10–11(1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3564–64.

76. Kerr, *A User's Guide*, *supra* note 18, at 1215; DOJ MANUAL, *supra* note 18, at 119.

"cloud computing,"[77] which can be used to slim down the computing requirements at the owner's end to simpler devices with low capacity hardware and only browser software. The Department of Justice has taken the position, usually successfully, that communications held by a "remote computing service" are not entitled to "super" warrant protection as in-transit communications, but rather have merely become records subject to simple subpoena or court order process.[78]

III. Guiding Cases

B. "Stored" or "In Transmission?"

Modern technologies for transmitting emails and text messages have created ambiguity in determining whether a particular access is to a communication in transit or when it is a stored communication. Emails and other messages may repose at points between origin by the sender and reception by the intended recipient; the status of messages once read but still retained has also been litigated.[79] If unlawful access occurs when a message is stored, then a criminal defendant cannot maintain that it should be excluded from evidence.[80] Civil damages for violation of the privacy protections under the ECPA are available both where the messages are stored and where they are still considered to be in transit, but, as noted

77. *Cloud Computing: Creating Value for Web 2.0 Apps*, http://www.vlab.org/article.html?aid=188 (last visited Oct. 22, 2009); Tim O'Reilly, *Web 2.0 and Cloud Computing*, Oct. 26, 3008, *available at* http://radar.oreilly.com/2008/10/web-20-and-cloud-computing.html.

78. DOJ MANUAL, *supra* note 12, at 120.

> However, this "either/or" approach to ECS and RCS is contrary to the language of the statute and its legislative history. The definitions of ECS and RCS are independent of each other, and therefore nothing prevents a service provider from providing both forms of service to a single customer. In addition, an email service provider is certainly an ECS, but the House report on the SCA also stated that an email stored after transmission would be protected by a provision of the SCA that protects contents of communications stored by an RCS. See H.R. Rep. No. 99-647, at 65 (1986). One subsequent court has rejected the Ninth Circuit's analysis in *Quon* and stated that a provider "may be deemed to provide both an ECS and an RCS to the same customer." Flagg, v. City of Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008). The key to determining whether the provider is an ECS or RCS is to ask what role the provider has played and is playing with respect to the communication in question.

79. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2004).

80. 18 U.S.C. §§ 2515, 2518(10)(a) (2006) (applying only to intercepted communications).

above, the cap on statutory damages is smaller for stored messages.[81] For stored messages, a plaintiff has also been required to show actual damages before being allowed to recover statutory damages at all.[82]

Because of the different treatment of messages, stored or not, courts have analyzed whether a message is considered stored at the following points in time: the period between the entry of keystrokes on a keyboard and the giving of the command "send" when the entered message is held in the internal memory of the sending computer;[83] the period during relayed transmission when the message packets are reassembled at an intermediary node and held briefly before being repacketized and sent on to the intended recipient;[84] the period during receipt by the intended recipient when the contents of the communication are displayed on a monitor simultaneously with being stored on a hard drive;[85] during access by remote examination of information stored on a hard drive, after intended recipient has viewed the contents;[86] during access to emails, including those unread by intended recipient, after unlawful seizure of computers of intended recipient;[87] and during access to viewed emails.[88]

In *United States v. Ropp*, the defendant was charged with interception under the Wiretap Act.[89] The defendant had installed a device, called a KeyKatcher, on the cable conducting electrical impulses from the keyboard to the central processing unit of a desktop computer normally operated by an insurance company employee.[90] The device would enable Ropp, upon recovery of the device, to access the content of all keystrokes made by the operator.[91] At the time the keystrokes were recorded, the computer was connected to the internet, but the message being composed on the

81. *See supra* note 57.

82. Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 208 (4th Cir. 2009).

83. United States v. Ropp, 347 F. Supp. 2d 831, 832 (C.D. Cal. 2004).

84. United States v. Councilman, 418 F.3d 67, 70 (1st Cir. 2005).

85. O'Brien v. O'Brien, 899 So.2d 1133, 1137 (5th Fla. Dist. Ct. App. 2005).

86. United States v. Steiger, 318 F.3d 1039, 1041–44 (11th Cir. 2003).

87. *See, e.g.*, Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461 (5th Cir. 1994); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 626 (E.D. Pa. 2001); Theofel v. Farey-Jones, 359 F.3d 1066, 1071–72 (9th Cir. 2004), *cert. denied*, 543 U.S. 813 (2004).

88. *See, e.g.*, Wesley College v. Pitts, 974 F. Supp. 375, 384 (D. Del. 1997); Garcia v. Haskett, No. C 05-3754 CW, 2006 U.S. Dist. LEXIS 46303, at *6–7 (N.D. Cal June 30, 2006).

89. United States v. Ropp, 347 F. Supp. 2d 831, 832 (C.D. Cal. 2004) (finding defendant guilty of a violation of 18 U.S.C. § 2511(1)(a)).

90. *Id.* at 831.

91. *Id.* at 832.

keyboard had not yet been "sent" with a command from the operator.[92] The court easily found that there had been an interception of an electronic signal, but focused its inquiry on whether the intercepted signals were an electronic communication protected by the Wiretap Act.[93] The relevant language for that analysis was in 18 U.S.C. § 2510(12): "whether the signals were transmitted 'by a system . . . that affects interstate or foreign commerce.'"[94]

U.S. District Court Judge Feess did not accept the Government's argument that the signals were transmitted to a system that affects interstate commerce simply because the computer was connected to the internet at the time, nor did he focus on the statutory jurisdictional element that the transmission be through a system that affects interstate commerce.[95] Instead, Judge Feess found that the signals were still internal to the computer itself, rather than being in transit.[96] The defendant's indictment under the Wiretap Act was dismissed because the judge found that there had been no interception of a communication because the information had not yet been sent.[97] In doing so, Judge Feess distinguished between interception of an electrical signal within a computer and interception of a communication in the process of transmission.[98] Although a later case has criticized the reasoning in *Ropp* in finding that interstate commerce was not involved, the latter judge did not reach the more fundamental question of whether the message being prepared was in a state of transmission before the "send" command was given.[99] In finding that the message was not in transmission, as well as not being in transmission in interstate commerce, Judge Feess relied heavily on the reasoning in the 2004 First Circuit decision in *United States v. Councilman*, which has subsequently been vacated and reversed after en banc review.[100] The *Councilman* case, discussed in more detail below, involved interception after the commencement of a transmission and therefore did not specifically apply to the issue in

92. *Id.* at 837.
93. *Id.* at 834.
94. *Id.*
95. *Id.* at 837.
96. *Id.* at 838.
97. *Id.* at 835 n.1.
98. *Id.* at 837.
99. Bramana v. Lembo, No. C-09-00106 RNW, 2009 U.S. Dist. LEXIS 42800, at *8 (N.D. Cal. May 20, 2009).
100. *Ropp*, 347 F. Supp. 2d at 836–37 (analyzing United States v. Councilman (*Councilman II*), 373 F.3d 197 (1st Cir. 2004); *vacated en banc*, *Councilman I*, 418 F.3d 67 (1st Cir. 2005)).

Ropp: the status of a message being prepared for transmission but not yet sent.

Significantly, Judge Feess analyzed the implications of a case where the Government had tailored its interception of keystrokes to mechanically separate those strokes when the computer was connected to a live internet connection from those entered when the computer was not so connected.[101] In that case, *United States v. Scarfo*, the keystrokes made when the computer was not connected were recorded.[102] Since the strokes were thus entirely within the computer system at that point, the interception was found not to violate the Wiretap Act, and therefore was not suppressed.[103]

Nevertheless, while *Scarfo* did not focus on the meaning of, and potential limitations inherent in, the definition of "electronic communication," it indicates the importance the trial court placed on determining whether the intercepted keystrokes were transmitted within, or beyond, the defendant's computer: Because the intercepted keystrokes were not transmitting beyond the computer, the trial court held that the provisions of the Wiretap Act did not apply.[104] However, the analysis in *Scarfo* did not clearly find that the message was not a communication in transmission at all because it had not been sent. Its language is equally consistent with finding transmission, but not in interstate commerce, so the Wiretap Act did not apply for jurisdictional reasons, even if the keystrokes being sent within the computer were part of the process of transmission that would otherwise be covered. Nevertheless, in applying the language of the statute in *Ropp*, Judge Feess concluded: "[t]hough the reasoning of *Scarfo* is flawed in some respects, its discussion of facts that are analogous to those presented in this case provides some support for the proposition that the transmission of signals within a computer do not constitute 'electronic communications' within the Act."[105]

In *Councilman*, the defendant was an officer for a company that dealt in rare books and provided email services to its subscribers, many of whom were rare book dealers.[106] Councilman was initially charged with unlawful interception of in-transit electronic

101. *Ropp*, 347 F. Supp. 2d at 835–36 (analyzing United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001)).

102. *Scarfo*, 180 F. Supp. 2d at 582.

103. *Id.*

104. *Id.*

105. *Ropp*, 347 F. Supp. 2d at 836.

106. *Councilman I*, 418 F.3d 67, 70 (1st Cir. 2005).

communications under the Wiretap Act because he had directed employees to intercept and copy incoming communications from Amazon.com to his customers, with the intent of giving his own service a competitive advantage.[107] The incoming messages were simultaneously sent on to the intended recipient and also copied to a mailbox for Councilman's employees to read.[108] The District Court reversed its initial denial of defendant's motion to dismiss after reevaluating the statutory language.[109] Guided by the reasoning of *Konop v. Hawaiian Airlines*, the court interpreted the statutory language to find that the Wiretap Act did not apply because the message was in storage on the server, albeit temporarily, at the time it was seized and copied.[110] A divided panel of the First Circuit affirmed the District Court,[111] but an en banc review subsequently reversed.[112] The First Circuit eventually held that the Wiretap Act applies when access is made to electronic communications *even* in storage, so long as the storage was *incidental* to transmission.[113] The court's reasoning has been described as developing a "contemporaneity" test for whether stored information is still in the process of transmission, which may be adopted by other courts in dealing with the difficult issue of whether emails that have been sent to the mailbox of the intended recipient, but are as yet unread, are still in the process of transmission, and thus protected under the Wiretap Act.[114]

The First Circuit's en banc majority opinion was written by Judge Lipez, who had dissented in the earlier proceeding.[115] Notably, he found that neither the plain meaning of the statute nor its legislative history were useful in deciding whether the defendant had violated the Wiretap Act, or merely the SCA, in obtaining copies of the contents of the transmission while it was in temporary storage:

107. *Id.* at 70–71.

108. *Id.* at 70.

109. United States v. Councilman (*Councilman III*), 245 F. Supp. 2d 319, 321 (D. Mass 2003).

110. *Id.* at 321 (interpreting Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002)).

111. *Councilman II*, 373 F.3d 197, 203–04 (1st Cir. 2004).

112. *Councilman I*, 418 F.3d 67, 69 (1st Cir. 2005).

113. *Id.* at 77, 85.

114. Michael D. Roundy, *The Wiretap Act – Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following* United States v. Councilman*'s Rejections of the Storage/Transit Dichotomy*, 28 W. NEW ENG. L. REV. 403, 425 (2006).

115. *Councilman I*, 418 F.3d at 69; *Councilman II*, 373 F.3d at 204.

> In short, the ECPA's plain text does not clearly state whether a communication is still an "electronic communication" within the scope of the Wiretap Act when it is in electronic storage during transmission. Applying canons of construction does not resolve the question. Given this continuing ambiguity, we turn to the legislative history.[116]

After a lengthy examination of legislative history, the *Councilman* majority concluded that it, too, was inconclusive on whether an email in temporary storage during transmission was covered by the Wiretap Act:

> If the addition of the electronic storage clause to the definition of "wire communication" was intended to remove electronic communications from the scope of the Wiretap Act for the brief instants during which they are in temporary storage en route to their destinations—which, as it turns out, are often the points where it is technologically easiest to intercept those communications—neither of the Senate co-sponsors saw fit to mention this to their colleagues, and no one, evidently, remarked upon it. No document or legislator ever suggested that the addition of the electronic storage clause to the definition of "wire communication" would take messages in electronic storage out of the definition of "electronic communication." Indeed, we doubt that Congress contemplated the existential oddity that Councilman's interpretation creates: messages-conceded by stipulation to be electronic communications-briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again. Cf. H.R.Rep. No. 99-647, at 35 ("[t]he term 'electronic communication' is intended to cover a broad range of communication activities.... Communications consisting solely of data... would be electronic communications.").
>
> In sum, the legislative history indicates that Congress included the electronic storage clause in the definition of "wire communication" provision for the sole reason that, without it, access to voicemail would have been regulated solely by the Stored Communications Act. Indeed, that is exactly what happened when Congress later removed the

116. *Councilman I*, 418 F.3d at 76.

> explicit reference to "electronic storage" from the definition of "wire communication" in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. . . .[117]

A 2005 civil case, *O'Brien v. O'Brien*, also used contemporaneity in determining whether messages were intercepted or merely accessed as a stored communication.[118] Mrs. O'Brien had placed software on a computer used by her husband to play Yahoo Dominoes with another woman.[119] Unknown to the husband, the software made copies of instant messages and email exchanges between the husband and the other woman, and saved them for later retrieval by the wife.[120] The husband sought to bar admission of the copies in their divorce case, arguing that it was illegally obtained.[121] The Florida statute involved[122] was similar to the federal Wiretap Act, so the judge expressly followed reasoning that has been applied to the Wiretap Act in coming to his conclusion that the messages were "intercepted" rather than merely retrieved from storage.[123]

> The Wife argues that the communications were in fact stored before acquisition because once the text image became visible on the screen, the communication was no longer in transit and, therefore, not subject to intercept. We disagree. We do not believe that this evanescent time period is sufficient to transform acquisition of the communications from a contemporaneous interception to retrieval from electronic storage. We conclude that because the spyware installed by the Wife intercepted the electronic communication contemporaneously with transmission, copied it, and routed the copy to a file in the computer's hard drive,

117. *Id.* at 78–79.

118. O'Brien v. O'Brien, 899 So.2d 1133, 1137 (5th Fla. Dist. Ct. App. 2005).

119. *Id.* at 1134.

120. *Id.*

121. *Id.*

122. FLA. STAT. § 934.02(3) (2003).

123. We discern that there is a rather fine distinction between what is transmitted as an electronic communication subject to interception and the storage of what has been previously communicated. It is here that we tread upon new ground. Because we have found no precedent rendered by the Florida courts that considers this distinction, and in light of the fact that the Act was modeled after the Federal Wiretap Act, we advert to decisions by the federal courts that have addressed this issue for guidance.

O'Brien, 899 So. 2d at 1135–36 (citations omitted).

the electronic communications were intercepted in violation of the Florida Act.[124]

The judge writing the *O'Brien* opinion expressly relied on the distinction between stored and in-transit communications that had been articulated by the Eleventh Circuit in *United States v. Steiger*.[125] Steiger was charged with sexual exploitation of children and child pornography crimes after an anonymous hacker had gained remote access to Steiger's computer.[126] Software placed on Steiger's computer allowed the hacker to examine Steiger's files; when disturbing images of child sexual abuse were found, the hacker anonymously contacted law enforcement officials, sending copies of the images together with identifying information that he had obtained from letters, banking records, and other data on Steiger's hard drive.[127] A government investigator checked the information and then obtained a search warrant for Steiger's computer, using as "probable cause" the information from the hacker and the corroborating and supplementary information learned from the investigation.[128]

Steiger sought to suppress the evidence from the hard drive of the computer, using two different lines of argument. He first argued that the search of his computer was a violation of the Constitutional prohibition against warrantless searches under the Fourth Amendment.[129] However, that would only apply if the search had been by the Government or its agent. The Fourth Amendment does not apply to searches by private persons. The Government was able to satisfy the court that the hacker had been operating independently, without the knowledge, much less the encouragement or support, of law enforcement officials, in searching Steiger's computer.[130] The court found no violation of Steiger's Fourth Amendment rights.[131]

124. *Id.* at 1137. The Florida statute, like the federal Wiretap Act, only provided an exclusion remedy for oral and wire communications, so the data communications that were intercepted by Mrs. O'Brien were not excludable under the statute. However, the appellate court held that the trial court had acted within the permissible zone of its general discretion in determining whether to admit evidence. *Id.* at 1137–38.

125. *Id.* at 1136–37 (analyzing United States v. Steiger, 318 F.3d 1039, 1047–52 (11th Cir. 2003)).

126. *Id.* at 1041.

127. *Id.* at 1042–44.

128. *Id.* at 1043.

129. *Id.* at 1045–46.

130. *Id.* at 1046.

131. *Id.* at 1045.

Steiger's second line of argument raised the issue of stored communications as compared to intercepted in-transit ones under the ECPA.[132] Here, the argument was that the acquisition and transmission of the information on Steiger's hard drive was an interception, and thus a violation of the Wiretap Act, which applies to private persons as well as to government officials.[133] Steiger then argued that illegally obtained evidence should be suppressed, even though the Wiretap Act expressly provides a suppression remedy only for unlawfully intercepted oral and wire communications.[134] His argument was based on 18 U.S.C. § 2517(3), which authorizes disclosure of electronic evidence at trial if it was acquired in accordance with the Wiretap Act, thus supporting the position that if it were not so acquired, it would not be admissible.[135]

The court ruled against both arguments, finding that the information accessed by the hacker was stored, not intercepted contemporaneously with transmission, and, in any event, that suppression was not available for electronic communications.[136] The *Steiger* court, quoting the reasoning developed through a line of cases and statutory changes, concluded that a violation of the Wiretap Act prohibition only would occur where the content of a message was accessed contemporaneously with transmission:

> By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of "intercept"—acquisition contemporaneous with transmission—with respect to wire communications. The purpose of the recent amendment was to reduce protection of voice mail messages to the lower level of protection provided other electronically stored communications. When Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term "intercept" with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make that definition applicable to voice mail messages as well. Congress, therefore, accepted and implicitly approved the judicial

132. *Id.* at 1046–47.
133. *Id.* at 1046.
134. *Id. See also* 18 U.S.C. §§ 2515, 2518(10)(a) (2006).
135. *Steiger*, 318 F.3d at 1046.
136. *Id.* at 1050–51.

> definition of "intercept" as acquisition contemporaneous with transmission.[137]

In addition to articulating the contemporaneity test for interception under the Wiretap Act, the *Steiger* court indicated the limitations of the SCA to address invasions of privacy that occur when messages stored on a home computer, even connected to the internet, are examined without authorization.[138]

> The SCA, however, does not appear to apply to the source's hacking into Steiger's computer to download images and identifying information stored on his hard-drive because there is no evidence to suggest that Steiger's computer maintained any "electronic communication service" as defined in 18 U.S.C. § 2510(15). We note, however that the SCA may apply to the extent the source accessed and retrieved any information stored with Steiger's Internet service provider. In sum, our reading of the Wiretap Act to cover only real-time interception of electronic communications, together with the apparent non-applicability of the SCA to hacking into personal computers to retrieve information stored therein, reveals a legislative hiatus in the current laws purporting to protect privacy in electronic communications. This hiatus creates no remedy.[139]

Thus, a distinction developed between data stored on home computers and communications held by third party internet service providers, which would be covered under the SCA, if at all. Within the home, the Fourth Amendment protections apply to limit intrusions on transmissions and stored communications by the government, but not by private persons. Communications held by third parties in the process of transmission would be protected from intrusion by both government and private persons under the Wiretap Act. Once the communications become stored, only the more limited protections of the SCA apply. In turn, those depend on the statutory

137. *Id.* at 1048 (quoting Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (citing Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994); United States v. Smith, 155 F.3d 1051 (9th Cir. 1998)).

138. *Id.* at 1049–51.

139. *Id.* at 1049 (citations omitted).

concept of "electronic communication service," developed more fully in *Quon v. Arch Wireless Operating Co.*, which is discussed below.[140]

In *Steve Jackson Games v. U.S. Secret Service,* a 1994 case that has been widely cited (although parts of the opinion have often been distinguished and criticized), the Fifth Circuit found a violation of the SCA when unread emails were accessed without authorization.[141] The court was clear that for interception under the Wiretap Act, contemporaneity would be relevant; thus, it found that unread emails in repose in the mailbox of the intended recipient were no longer subject to such interception.[142] However, the SCA does provide at least some level of protection, so long as the email or other communication is being held by an entity qualifying under the SCA as an "electronic communications service."[143]

In *Steve Jackson Games*, the SCA applied to information stored on a secure website accessed by third-party users.[144] In *Konop*, the SCA was held to be applicable to information stored on an electronic bulletin board service.[145] Communications stored on a home computer, as in *Steiger*, would be protected by Fourth Amendment process, rather than under the ECPA, although some courts have strained to find that a home computer could be an "electronic communications service."[146]

One controversial decision in the Ninth Circuit found that read emails stored on an electronic communications service were protected indefinitely, being in electronic storage for backup protection.[147] Even then, the court recognized that there was contrary authority that has found only unread email to be protected in electronic storage because they are still incidental to transmission.[148]

140. Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), *petition for rehearing en banc denied*, 554 F.3d 769 (9th Cir. 2009) case divided into public and private causes of action, *cert. granted*, City of Ontario, CA v. Quon, 130 S. Ct. 1011 (2009) *cert. denied*, USA Mobility Wireless, Inc. v. Quon, 130 S. Ct. 1011 (2009).

141. Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 462–63 (5th Cir. 1994).

142. *Id.* at 460, 463.

143. *See* DOJ MANUAL, *supra* note 12, at 117–19, 133–34 (explaining 18 U.S.C. § 2703(a)).

144. *Steve Jackson Games*, 36 F.3d at 462–64.

145. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 872 (9th Cir. 2002).

146. Kerr, *A User's Guide, supra* note 18, at 1214–15.

147. Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (citing 18 U.S.C. § 2510(17)(B)), *cert. denied*, 543 U.S. 813 (2004) *criticized at* Kerr, *A User's Guide, supra* note 18, at 1217–18.

148. *Theofel*, 359 F.3d at 1075 (citing cases that have interpreted 18 U.S.C. § 2510(17)(A)).

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.[149]

The Department of Justice ("DOJ") takes the position that after an email message has been read, it may no longer be protected as a communication stored at an electronic communications service, although the SCA does distinguish between communications stored with a remote computing service and those stored with a third party that provides internet service for electronic communications.[150] According to the DOJ's reasoning, once the recipient retrieves the e-mail, however, the communication reaches its final destination.[151] If a recipient then chooses to retain a copy of the accessed communication on the provider's system, because the process of transmission to the intended recipient has been completed, the copy is simply a remotely stored file.[152]

C. Privacy Protection Varies with the Location and Function of the Place of Storage

In addition to the time point in determining whether a particular communication is in transit or stored, the legislation also sets up different treatment that turns on the nature of the entity holding a stored communication. Communications in storage at an "electronic communications service," such as Yahoo! or Gmail, would be protected by requiring a warrant based on probable cause, under independent judicial supervision, for access by law enforcement

149. *Id.*

150. DOJ MANUAL, *supra* note 12, at 123–24.

151. *Id.* at 124.

152. *Id.* (citing Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2004) (finding that an e-mail acquired from post-transmission storage was not in "electronic storage" so its acquisition was not a violation of the Wiretap Act)). Contrary to the *Theofel* holding, the DOJ cites H.R. REP. No. 99-647, at 64–65 (1986), as "noting Congressional intent that opened e-mail left on a provider's system be covered by provisions of the SCA relating to remote computing services, rather than provisions relating communications in 'electronic storage.'" *Id.*

agents;[153] as noted above, a Wiretap Act "super" warrant is not required because the communications are stored. If the storage is in a "remote computing service," access is even less protected, needing only a subpoena or court order to obtain access.[154] When the ECPA was enacted, it was a common practice for enterprises to transmit data to such "remote computing services" which would provide a level of computing power that was generally too expensive at the time for each user to own and maintain.[155] Centralized servers would hold the data and provide operations that required that level of computing power, such as calculation and database functions.[156] That pattern of operations changed dramatically in the two decades after the ECPA as the price of computing power fell dramatically and more user-friendly software interfaces permitted data handling by operators with less skill.[157] However the current shift toward cloud computing would again locate data, including stored communications, in entities that would hold them as a "remote computing service." Even under long-established patterns of usage, multiservice entities are popular that provide not only transmission of email initially but also storage, ready retrieval and searching, and integration with other services, such as Google's Gmail. The provision of such a range of services leaves ambiguous the intent of the recipient of the message in placing, or in not removing, a communication held by that entity. When read email is left in one's account with Gmail, for example, the intent may be to use it as data for retrieval by the Google search engines, rather than to hold it as a backup for the initial communication. In addition to communications held on third-party computers, privacy protection issues have arisen for those held on home computers and on personal devices, particularly including cellphones and other portable communications devices, such as netbook computers.[158]

In cases where delivered and stored, or unread, email has been accessed within a privately-held system, courts have looked at the

153. 18 U.S.C. § 2703(a) (2006).

154. 18 U.S.C. § 2703(b) (2006).

155. Kerr, *A User's Guide*, *supra* note 18, at 1213–14.

156. *Id.* at 1214.

157. *See, e.g.*, Helpdesk Pro, Web-Based Customer Service Software—the benefits of choosing web enabled applications, http://www.helpdeskpro.net/web-based_software.htm (last visited Apr. 5, 2010). *See also* Dillard Boland, et al., *How Emerging Technologies are Changing the Rules of Spacecraft Ground Support*, Space Mission Operations and Ground Data Sys. – SpaceOps '96, EUROPEAN SPACE AGENCY, 328, 332 (1996), *available at* http://articles.adsabs.harvard.edu/full/1996ESASP.394..328B/ 0000328.000.html.

158. *See* Klump v. Nazareth Area Sch. Dist., 425 F. Supp. 2d 622 (E.D. Pa. 2006). *See also infra* note 185.

"facility" language in the SCA to find whether such access would be actionable.[159] The SCA provides some protection for information held by a "remote computing service" and greater protection when the information is in an "electronic communication service." The distinction in protections between these two types of services was highlighted in the 2008 Ninth Circuit case, *Quon v. Arch Wireless Operating Co.*[160] There, the court examined the role of the ISP to see whether it held stored messages as an electronic communication service or if it functioned as an remote computing service.[161] If Arch, the third party ISP, was holding the messages as an electronic communication service, then plaintiff Quon could maintain a civil action for violation of the SCA because Arch had released the content of the message to the employer, which was paying for the service, since the employer was not the addressee.[162]

Even if the facility is one where protection against access is provided, a violation of the SCA may not be found merely because someone has access to one's emails and other electronic communications in storage: the scope of authority for access will be examined as well. Parties to the communication have authority not only to access stored communications themselves, but also to give others permission to do so.[163] In a 2002 Ninth Circuit case, *Konop v.*

159. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002) (discussing authorized access to stored communications through a "user"); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 309 (E.D.N.Y. 2005) (examining the "electronic communication service" limitations of the SCA). In *JetBlue*, the airline's computerized reservation system was held not to be an ECS; although customers could use the airline's system to transmit data, the airline itself was not a provider of electronic communication services, but rather was a consumer of such services. *In re JetBlue Airways*, 379 F. Supp. 2d at 309. Therefore the airline could not be held liable for its alleged disclosure of customer records. *Id.* at 310. *See also* Garcia v. Haskett, No. C 05-3754 CW, 2006 U.S. Dist. LEXIS 46303, at *11–14 (N.D. Cal June 30, 2006) (further developing the definition of an electronic communications system stated in *JetBlue*). "According to the Complaint, the Partnership is a limited liability partnership engaged in the practice of law, and it purchases electronic communication services through Tri-Valley; it is not a 'facility through which an electronic communication service is provided.'" *Id.* at *13.

160. Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), *petition for rehearing en banc denied*, 554 F.3d 769 (9th Cir. 2009) case divided into public and private causes of action, *cert. granted*, City of Ontario, CA v. Quon, 130 S. Ct. 1011 (2009) *cert. denied*, USA Mobility Wireless, Inc. v. Quon, 130 S. Ct. 1011 (2009).

161. *Id.* at 900.

162. *Id.* at 900; 18 U.S.C. § 2702(b)(3) (2006).

163. 18 U.S.C. § 2702(b)(1) (2006) permits service providers to disclose the contents of stored communications "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2702(b)(3) permits a similar exception with respect to remote computing services. Under 18 U.S.C. § 2701(c)(2) (2006), a "user" of the service can authorize a third party's access to the communication.

Hawaiian Airlines,[164] an employee who himself had permission to access a protected bulletin board website, which was intended only for employees, could authorize his employer to access the information, even against the express terms of the poster of the data.[165] Both *Quon* and *Konop* are discussed in more detail below.

In *Quon*, the communications were records of data transmissions over pagers provided by the city to police officers.[166] There was a monthly cap on the transmissions, which Officer Quon and others exceeded from time to time.[167] Department policies were in place, and signed by the officers, retaining the right of the department to look at communications and specifically warning the officers that they should have no expectation of privacy in the communications.[168] However, the officer in charge of handling the overage situation assured Quon that he did not want to get into the auditing business and that, if Quon simply paid the overage each month as a personal expense, he would not do so.[169] Quon in fact paid the overage on several occasions.[170]

The Ninth Circuit analyzed the application of the Fourth Amendment protections.[171] It found that Quon would be able to bring a claim against the city to argue that he did have an expectation of privacy because of the assurance of the officer in charge and past practice, even in the face of the policy.[172] Thus for a claim based on a violation of Constitutionally-protected privacy rights, the court found that Quon could proceed to the next step, a "reasonableness" inquiry:

> Under the "general Fourth Amendment approach," we examine "the totality of the circumstances to determine whether a search is reasonable." . . . "The reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[173]

164. *Konop*, 302 F.3d at 879–80.
165. *Id.*
166. *Quon*, 529 F.3d at 898.
167. *Id.* at 897.
168. *Id.* at 896.
169. *Id.* at 897.
170. *Id.*
171. *Id.* at 903.
172. *Id.*
173. *Id.* (citing United States v. Knights, 534 U.S. 112, 118–19 (2001)).

The claim under the SCA was against the provider, Arch Wireless Operating Co., charging that it violated Quon's rights in releasing the contents of the messages to the city when the city requested them.[174] The communications were heavily of a personal nature, involving specific sexual references.[175] Under the SCA, to receive the higher degree of protection, the communication must be held by an electronic communication service in "electronic storage":

> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . .[176]

However, the SCA has exceptions carved into it for voluntary disclosures of communications:

> A provider described in subsection (a) may divulge the contents of a communication—(1) to an addressee or . . . (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service . . . .[177]

If Arch's activities made it an "electronic communications system," then the messages were protected from disclosure without Quon's permission. However, if Arch were acting as merely a "remote computing service," then it would not be liable for turning over the content to its subscriber, the city, who was paying for the service.[178]

Under the language of the statute, an electronic communication service "provides to users thereof the ability to send or receive wire or electronic communications."[179] The text messaging pager services provided by Arch would likely meet that definition. A remote

174. *Id.* at 902.
175. *Id.* at 898.
176. 18 U.S.C. § 2702(a) (2006).
177. 18 U.S.C. § 2702(b) (2006).
178. *Quon*, 529 F.3d at 895–96.
179. 18 U.S.C. § 2510(15) (2006).

computing service provides "computer storage or processing services by means of an electronic communications system."[180] Arch did store messages, both temporarily, pending retrieval by the addressee, and archivally.[181] However the Ninth Circuit did not hesitate to find Arch to be an electronic communication service noting that "Congress contemplated this exact function could be performed by an electronic communication service as well, stating that an electronic communication service would provide (A) temporary storage incidental to the communication; and (B) storage for backup protection."[182]

Although the court went on to acknowledge that information going to and from a remote computing service would travel through an electronic communications system, it concluded that a remote computing service was a facility whose dominant function was either storage or sophisticated offsite data processing for its clients.[183] Therefore, the Ninth Circuit held that "[w]hen Arch Wireless knowingly turned over the text messaging transcripts to the City, which was a 'subscriber,' not 'an addressee or intended recipient of such communication,' it violated the SCA."[184]

Text messages, such as those involved in *Quon*, have become a major mode for communications, and therefore the degree of protection for privacy in them has begun to be examined by courts in actions under the Wiretap Act, the SCA, and their state law analogues.[185]

In a 2006 District of Columbia case, *United States v. Jones*, U.S. District Judge Ellen Segal Huvelle found that the Wiretap Act does not apply to the government's acquisition of text messages held in storage at electronic communication service providers; therefore, it was held that the more stringent requirement of "necessity" for issuing a search warrant required by the Wiretap Act does not apply to such communications.[186] She summarized a line of cases to

180. 18 U.S.C. § 2711(2) (2006).

181. *Quon*, 529 F.3d at 901.

182. *Id.* (quoting 18 U.S.C. § 2510(17)).

183. *Id.* at 902.

184. *Id.* at 903.

185. Nicole Cohen, *Using Instant Messages as Evidence to Convict Criminals in Light of National Security: Issues of Privacy and Authentication*, 32 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 313, 313 n.3 (2005).

186. United States v. Jones, 451 F. Supp. 2d 71, 75–76 (D.D.C. 2006).

conclude that the text messages were held in storage and thus covered under the SCA.[187]

The extent to which telephone companies and other providers of messaging services archive messages is not clear.[188] However, law enforcement officials and reporters using Freedom of Information Act requests have been able to obtain the content of messages, as opposed to mere "addressing" information, in cases that have been reported in the news.[189]

An alternative argument under facts parallel to those in *Quon* is presented in a recent court holding that text messages by public servants on their government-provided pagers are public records, not protected by privacy claims at all.[190] About 1,400 text messages between former Detroit mayor Kwame Kilpatrick and his former aide Christine Beatty were ordered released in an action brought by the *Detroit Free Press* and the *Detroit News*.[191] Another request for the messages as evidence was granted in a civil federal court case in Detroit stemming from the murder of an exotic dancer.[192] Among a great deal of scandal, it was charged that the investigation was

187. *Id.*

188. *See* Marcus R. Jones & Hugh H. Makens, *Traps in Electronic Communications*, 8 J. BUS. & SEC. L. 157 (2008).

> Text messages are a particularly difficult subject because they do not reside on a company's server system. The way most text messaging works is that messages are sent from one user's phone through cellular phone towers to the recipient user's phone. The messages reside in the memory of each user's phone. Therefore, centralized storage of such messages is difficult without controlling the user's phone. IM's work the same way in that normally each individual computer stores the messages and the user may choose to delete the message trail upon exit of the application. However, because the messages go through a gateway it is possible for a company to store and retrieve such messages. In fact, many vendors are actively touting this ability. However, many companies have decided that they cannot preserve IM communications and have prohibited their use.

Id. at 162.

189. *See, e.g.*, Joe Swickard, *Steps in the Text Message Scandal*, DETROIT FREE PRESS, Mar. 10, 2009, *available at* http://www.freep.com/article/20090310/NEWS01/903100351/Steps-in-the-text- message-scandal.

190. M. Elrick, *Judge Rules that Kilpatrick, Beatty Texts are Public Record*, DETROIT FREE PRESS, Mar. 4, 2009, *available at* http://www.freep.com/article/20090304/NEWS01/90303093/Judge-rules-that-Kilpatrick--Beatty-texts-are-public-record.

191. *Id.*

192. Flagg v. City of Detroit, No. 05-74253, 2009 U.S. Dist. LEXIS 106459, at *5–6 (E.D. Mich. Nov. 16, 2009).

compromised for political reasons; one of the defense attorneys unsuccessfully argued that the SCA protects text messages from discovery in civil actions more than it does in criminal proceedings.[193]

Both private parties and law enforcement officials have introduced text message information as evidence in criminal trials. In a recent tragic Ontario, Canada case, the prosecution introduced 30,000 pages, including months of chat sessions and text messages, between the accused and her boyfriend, both high school students, as evidence that the young woman was guilty of murder in inciting her boyfriend to stab a 14-year-old student to death.[194] The evidence was damning and both young people were convicted after jury trials.[195] In a murder case in Texas, cell phone and text messaging records during the time of the murders were part of the evidence that ultimately led to a conviction.[196] However, the summary information available in that situation suggests that the messaging records were location-based in nature, more like the "addressing" information that is not afforded privacy protections, rather than content which might have more protections, and is somewhat less likely to be preserved by carriers.[197]

In *Klump v. Nazareth Area School District*, school officials were defendants in a civil case for invasion of privacy of a student for accessing stored messages on his cell phone.[198] The 2006 case was brought under Pennsylvania's Wiretapping and Electronic Surveillance Control Act.[199] A high school student had his cell phone

193. Paul Egan, *Federal Judge May Release Text Messages*, THE DETROIT NEWS, Mar. 25, 2009, *available at* http://www.detnews.com/article/20090325/METRO01/903250378.

194. Brian Gray, *Accused's Messages Led to Rengel's Murder: Crown 'I Want Her Dead,'* TORONTO SUN, Mar. 17, 2009, *available at* http://www.torontosun.com/news/torontoandgta/2009 /03/17/8774781-sun.html; *Jury in Rengel Murder Trial Deliberates for 3rd Day*, CBC NEWS, Mar. 20, 2009, *available at* http://www.cbc.ca/canada/toronto/story/2009/03/20/rengel-trial.html; Rosie Dimano, *Rengel Defendant Venomous and Vulgar*, TORONTO STAR, Mar. 20, 2009, *available at* http://www.thestar.com/article/605355.

195. Natalie Alcoba, *Life Sentence for Stefanie Rengel's Killer*, NATIONAL POST, Sept. 28, 2009, *available at* http://network.nationalpost.com/NP/blogs/toronto/archive/2009/09/28/stefanie-rengel-s-killer-faces-sentencing.aspx.

196. Brad Kellar, *Woodruff Trial Underway in Hunt County*, THE HERALD BANNER, Mar. 12, 2009, *available at* http://rockwallheraldbanner.com/local/x1054522157/Woodruff-trial-underway-in-Hunt-County; Richard Abshire, *Man Found Guilty of 2005 Murder of his Parents in Hunt County*, THE DALLAS MORNING NEWS, Mar. 21, 2009, *available at* http://www.dallasnews.com/sharedcontent/dws/news/ localnews/stories/DN-woodruff_21met.ART.State.Edition2.4ad7cc5.html.

197. Kellar, *supra* note 196.

198. Klump v. Nazareth Area Sch. Dist., 425 F. Supp. 2d 622, 627–28 (E.D. Pa. 2006).

199. *Id.* at 627 (citing 18 PA. CONS. STAT. ANN. §§ 5703, 5741 (1988) (Pennsylvania's equivalent of the Wiretap Act and the SCA, respectively).

confiscated by school authorities who then accessed his stored text messages and voice mail in search of evidence that the student was dealing in drugs.[200] The court found that the student could assert a claim under the Pennsylvania statute for access to stored messages, but distinguished the school authorities' interception of incoming text messages.[201] It found that the recipient had no standing for a claim of interception, although the sender might.[202] The court concluded that both the sender and the recipient would have standing to claim invasion of privacy with respect to the stored messages.[203] Following federal practice, the claims based on the access to the student's phone call log and number directory were found to be mere addressing information, not "communication" that is protected under the communications privacy legislation.[204]

D. Constitutional Protection for Interceptions Otherwise Violating the Wiretap Act

The preceding cases spotlight the "public/private" line in information, with many similar cases and debates in the news.[205] One of the most fiercely litigated cases challenged the Supreme Court's holding in *Bartnicki v. Vopper*[206] that the wiretapping laws violate the First Amendment when they outlaw all disclosures of intercepted information, notably when the contents of the intercepted communication concern a matter of public debate. That case, *Boehner v. McDermott*, began with a 1996 conference call by cell phone among prominent Republican politicians, one of whom was then House Speaker, Newt Gingrich.[207] The discussion involved orchestrating a response to an ethics investigation; the cell phone broadcast (a radio transmission) was picked up by a nearby Democrat couple with a scanner and tape recorder, who just happened to have them on hand.[208] Scanning and recording, despite its illegality, had been popularized after 1992, when Princess Diana's conversation with

200. *Id.* at 630–31.

201. *Id.* at 633–34.

202. *Id.* at 633.

203. *Id.* at 628.

204. *Id.*

205. *See, e.g.*, The Associated Press, *States fight to keep officials' email from public inspection*, Mar. 19, 2008, *available at* http://www.firstamendmentcenter.org/news.aspx?id=19816.

206. Bartnicki v. Vopper, 532 U.S. 514, 544 (2001).

207. Boehner v. McDermott, 484 F.3d 573, 575 (D.C. Cir. 2007), *cert. denied*, 128 S. Ct. 712 (2007).

208. *Id.*

her male friend on a cell phone had allegedly been picked up and appeared in the British media.[209] The recorded Gingrich conversation found its way into the hands of the ranking Democrat on the House Ethics Committee, Rep. James A. McDermott of Washington state.[210] Subsequently, the recording was released to the press.[211]

The tapers were charged with a criminal violation of the Wiretap Act.[212] They pled guilty and were assessed a $500 fine.[213] However, the larger issue was raised when the politician whose cell phone had been targeted, Rep. John Boehner, brought a civil action against McDermott under The Wiretap Act and its Florida equivalent.[214] The politically sensitive and heavily financed case worked its way through the courts and appeals processes, with First Amendment arguments raised by the Democrats (public figure, truthful information disclosed, McDermott acquired the information without illegal action).[215] The Republican counterargument centered on the conceded illegality of the initial recording of the information, as a violation of the Wiretap Act, and the likelihood that McDermott knew of that illegality when he allowed for release of the information.[216]

On its final appeal, upon rehearing en banc, the Court of Appeals for the D.C. Circuit issued a split decision, but ultimately affirmed summary judgment for Boehner, finding that the First Amendment should not protect McDermott from civil liability.[217] However, the dissent, speaking for a majority in one part, held that *Bartnicki* is controlling in that the government cannot silence information of public concern when the discloser came upon the information without illegal actions.[218]

209. Nick Allen & Gordon Rayner, *Diana's Squidgygate tapes 'leaked by GCHQ'*, THE TELEGRAPH, Jan. 11, 2008, *available at* http://www.telegraph.co.uk/news/uknews/1575117/Dianas-Squidgygate-tapes-leaked-by-GCHQ.html.

210. *Boehner,* 484 F.3d at 576.

211. *Id.*

212. *Id.* at 577.

213. *Id.*

214. Boehner v. McDermott, Civ. No. 98-594(TFH), 1998 U.S. Dist. LEXIS 11509, at *5–6 (D.D.C. July 27, 1998).

215. *Boehner,* 484 F.3d at 577.

216. *Id.*

217. *Id.* at 579–80.

218. *Id.* at 586.

IV. Conclusion

The rationale for distinguishing between transmission and storage in general emerges within the historical pattern of the federal interest in privacy protection. The Wiretap Act antedated the 1986 ECPA,[219] and is now incorporated within it. Under the initial version of the act, Congress created a framework for protecting telephone communications from interception by law enforcement officials.[220] All telephone communications in that era were uttered by the human voice and received contemporaneously by the hearer.[221] The ECPA extended the Wiretap Act to include data communications but, as we have seen, human voice communications are protected by a stronger enforcement mechanism than that provided for violations intercepting non-voice communications,[222] although both have a higher degree of protection than such communications when considered "stored." Western cultural tradition, dating back at least to Socrates, treats oral communications with more deference than written ones:

> even the best of writings are but a reminiscence of what we know, and that only in principles of justice and goodness and nobility taught and communicated orally for the sake of instruction and graven in the soul, which is the true way of writing, is there clearness and perfection and seriousness . . . .[223]

Fixation and retrieval mechanisms could be a basis for that tradition, as suggested in the Phaedrus.[224]

---

219. The Wiretap Act was initially enacted June 19, 1968, P.L. 90-351, Title III, § 802, 82 Stat. 212. Antedating it, § 605 of the Federal Communications Act of 1934, 48 Stat. 1103 (1934), "prohibited the 'interception' and 'divulgence' or 'use' of the contents of a wire communication. At passage of the Act, managers of the bill observed, '[I]t does not change existing law.'" 78 CONG. REC. 1013 (1934), cited in Memorandum of November 3, 1971, to Senator John L. McClellan from G. Robert Blakey, Chief Counsel, Subcommittee on Criminal Laws and Procedures, *available at* http://www.gpoaccess.gov/congress/senate/judiciary/sh92-69-267/249-252.pdf.

220. The Wiretap Act, P.L. 90-351, Title III, § 802, 82 Stat. 212 (1968).

221. *Id.*

222. *See, e.g.*, 18 U.S.C. § 2515 (2006) (providing suppression remedy only for wire and oral communications, but not data communications).

223. PLATO, PHAEDRUS (Benjamin Jowett trans.) (360 B.C.E.), *available at* http://classics.mit. edu/Plato/phaedrus.html.

224.

> But when they came to letters, This, said Theuth, will make the Egyptians wiser and give them better memories; it is a specific both for

the memory and for the wit. Thamus replied: O most ingenious Theuth, the parent or inventor of an art is not always the best judge of the utility or inutility of his own inventions to the users of them. And in this instance, you who are the father of letters, from a paternal love of your own children have been led to attribute to them a quality which they cannot have; for this discovery of yours will create forgetfulness in the learners' souls, because they will not use their memories; they will trust to the external written characters and not remember of themselves. The specific which you have discovered is an aid not to memory, but to reminiscence, and you give your disciples not truth, but only the semblance of truth; they will be hearers of many things and will have learned nothing; they will appear to be omniscient and will generally know nothing; they will be tiresome company, having the show of wisdom without the reality.

Phaedr. Yes, Socrates, you can easily invent tales of Egypt, or of any other country.

Soc. There was a tradition in the temple of Dodona that oaks first gave prophetic utterances. The men of old, unlike in their simplicity to young philosophy, deemed that if they heard the truth even from "oak or rock," it was enough for them; whereas you seem to consider not whether a thing is or is not true, but who the speaker is and from what country the tale comes.

Phaedr. I acknowledge the justice of your rebuke; and I think that the Theban is right in his view about letters.

Soc. He would be a very simple person, and quite a stranger to the oracles of Thamus or Ammon, who should leave in writing or receive in writing any art under the idea that the written word would be intelligible or certain; or who deemed that writing was at all better than knowledge and recollection of the same matters?

* * *

to "write" his thoughts "in water" with pen and ink, sowing words which can neither speak for themselves nor teach the truth adequately to others?

Phaedr. No, that is not likely.

Soc. No, that is not likely—in the garden of letters he will sow and plant, but only for the sake of recreation and amusement; he will write them down as memorials to be treasured against the forgetfulness of old age, by himself, or by any other old man who is treading the same path. He will rejoice in beholding their tender growth; and while others are refreshing their souls with banqueting and the like, this will be the pastime in which his days are spent.

Phaedr. A pastime, Socrates, as noble as the other is ignoble, the pastime of a man who can be amused by serious talk, and can discourse merrily about justice and the like.

Oral communications address a known audience in the speaker's immediate presence, rather than future viewing by an unknown audience. The traditional law school teaching technique of "Socratic" dialogue recognizes the value of incorporating into the communication the speaker's fund of information and organizational structures held concurrently in the speaker's memory, rather than located in written sources used to refresh memory. However, in the past, writings have been organized in linear mode, and disparate writings might be connected chronologically while writings related in subject matter would not be aggregated systematically.[225] By contrast, modern digital technologies and installations, such as Google's software and server farms, collect immense archives of data, including communications, and search techniques allow us to retrieve it, using tailored aggregation filters, at the speed of light.[226] Hyperlinking and other nonlinear techniques of expression may challenge the Socratic analysis.

> Soc. True, Phaedrus. But nobler far is the serious pursuit of the dialectician, who, finding a congenial soul, by the help of science sows and plants therein words which are able to help themselves and him who planted them, and are not unfruitful, but have in them a seed which others brought up in different soils render immortal, making the possessors of it happy to the utmost extent of human happiness."

Id.

225. Allan Kotmel, *Hypertext vs. Papertext: Linear vs. Non-Linear*, Rensselaer Polytechnic Institute, 1996, http://www.rpi.edu/dept/llc/webclass/web/filigree/kotmel/linear.html (last visited Mar. 26, 2010). For example,

> there are many different linear paths through the networked content; that the content is often created in a 'linear mode' – that is, I have read through a series of posts, comments [sic] etc, in some sort [sic] order then add my own; that the time order in which content is created is not necessarily the order in which it will be read (for example, suppose post A and B were written yesterday, independently of and in ignorance of each other; I post a comment C to A that furthers the argument A and then links and leads into B which takes the argument yet further; the linear reading order is ACB; the content creation order could have been ABC or BAC).
>
> To a certain extent, there is an element of luck involved in the path a reader takes as they click through a linked network of resources.

Comment of Tony Hirst to OUseful.Info, the blog, http://ouseful.wordpress.com /2009/01/30/non-linear-uncourses-time-for-linked-ed/ (Jan. 31, 2009, 12:31 PM).

226. Luiz André Barroso, Jeffrey Dean, & Urs Hölzle, *Web Search for a Planet: The Google Cluster Architecture*, IEEE COMPUTER SOC'Y, Mar.–Apr. 2003, at 23–24, *available at* http://labs.google.com/papers/googlecluster-ieee.pdf.

A lesser value attaching to communications that are "fixed" in writing, such as text messages or email, would support the statutory framework privileging oral/aural communications over written ones. Professor Orin S. Kerr, who has written extensively on the SCA,[227] suggests that the difference in treatment is based on the technical means by which the intrusion is accomplished: that interceptions of oral and wire communications require ongoing surveillance of the communication medium, while investigation of a stored communication requires only seeking and obtaining the target communication itself.[228] However, that does not adequately address the higher protection given to oral/aural communications in transmission as compared to data communications in transmission. On the other hand, both the data transmission and the data in storage are fixed in writing. Perhaps the connection should be drawn between the immediate "fixation" in the email or text message and the more enduring "fixation" that "storage" implies. The contemporaneity of oral/aural interchange may thus be seen as analogous to the exchange provided by "contemporaneity" that the case law has developed as the defining element of "transmission" as distinct from "storage." Thus, the privileging of in-transit data communications over stored communications would be based, not on an expectation of privacy in the ephemeral spoken word, but rather in the nature of contemporaneous communication as compared to that which has been not only fixed, but also stored away, far from its initial context or the opportunity for the participants in the communication to amplify or correct understanding by discourse.

The absence of philosophical insight, the ambiguity and sketchiness of legislative guidance, and the complexity of the statutory language have resulted in cases defining "storage" under the SCA, and thus delimiting privacy protections, that have been fairly described as "incoherent and arbitrary" by Professor Kerr.[229] Professor Kerr has suggested that providing an exclusionary rule for violations of the SCA would lead to more clarity.[230] However, if the exclusionary remedy is not available for violations of the SCA, the result is likely to be greater privacy protection in the civil claims cases. The analysis in civil cases, as in *O'Brien* and *Konop*, relies

227. Kerr, *Lifting the "Fog," supra* note 48; Kerr, *A User's Guide, supra* note 18.
228. Kerr, *A User's Guide, supra* note 18, at 1231.
229. *Id.* at 1233.
230. *Id.* at 1241.

heavily on definitions developed in the criminal context.[231] Continuing to confine the exclusion remedy to violations involving transmission of communications of the human voice, rather than data in transit and storage, would reduce prosecutorial pressure on courts to allow credible evidence obtained in criminal cases by means that are challenged as violating privacy protections. Thus, the zone of protection for data and stored communications would not be reduced by borderline cases.

Professor Kerr has also suggested that the Computer Fraud and Abuse Act should be used as the basis for criminal prosecution of intrusions into stored communications and that the criminal provision of the SCA be repealed as redundant and confusing.[232] However, a strong case can be made that Congress should instead repeal the provision of a civil remedy for violations of both the Wiretap Act and the SCA. The interpretational eddies and cross-currents that have resulted from applying the same statutory language in the different contexts of civil and criminal cases could thus be avoided. Retaining federal criminal provisions while eliminating the civil claim remedies would still provide a unified federal approach to set a baseline for protecting electronic communications. State laws provide civil remedies for privacy intrusions. The provision of civil remedies in federal criminal legislation should be cautiously evaluated in view of their potential to clog federal court dockets, and to extend federal control and restrictions over tort-like litigation and remedies, without a specific examination of the issues that such extension raises.

231. O'Brien v. O'Brien, 899 So.2d 1133, 1134–35 (5th Fla. Dist. Ct. App. 2005); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir.2002).

232. Kerr, *A User's Guide*, *supra* note 18, at 1239–40. Repealing expansive criminal provisions in federal legislation has been widely advocated in the past decade. *See generally* William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505 (2001); John S. Baker, Jr., *Measuring the Explosive Growth of Federal Crime Legislation*, THE FEDERALIST SOC'Y (Oct. 2004), *available at* http://www.fed-soc.org/doclib/20080313_CorpsBaker.pdf; Erik Luna, *The Overcriminalization Phenomenon*, 54 AM. U.L. REV. 703 (2005); Brian Walsh, *Doing Violence to the Law: The Over-Federalization of Crime*, 20 FED. SENT'G REP. 295 (June 2008).

* * *